(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2001－520775
（P2001－520775A）
(43)公表日　平成13年10月30日(2001.10.30)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　7/72		Ｇ０６Ｆ	7/72	
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ａ ６５０Ｚ

審査請求　未請求　予備審査請求　有　（全 37 頁）

(21)出願番号　特願平10－544618
(86)(22)出願日　平成10年４月20日(1998.4.20)
(85)翻訳文提出日　平成11年10月18日(1999.10.18)
(86)国際出願番号　ＰＣＴ／ＣＡ９８／００４６７
(87)国際公開番号　ＷＯ９８／４８３４５
(87)国際公開日　平成10年10月29日(1998.10.29)
(31)優先権主張番号　９７０７８６１．２
(32)優先日　平成９年４月18日(1997.4.18)
(33)優先権主張国　イギリス（ＧＢ）

(71)出願人　サーティカム　コーポレイション
カナダ，オンタリオ州　エル４ダブリュー　５エル１，ミシソーガ　フォース　フロア，エクスプローラー　ドライブ　5520
(72)発明者　バンストーン，スコット，エイ．
カナダ　エヌ２ティー　２エイチ４　オンタリオ　ワーテルロー　サンドブロック　コート　539
(72)発明者　ランベルト，ロバート，ジェイ．
カナダ　エヌ２エル　３ビー８　オンタリオ　ワーテルロー　ナンバー　212　シーグラム　ドライブ　106
(74)代理人　弁理士　谷　義一　（外２名）

最終頁に続く

(54)【発明の名称】　算術プロセッサ

(57)【要約】
この開示は、有限体演算やモジュラ整数演算など一群の関連する算術演算をそれぞれパフォームする複数の算術回路を有するＡＬＵを含むことを特徴とする算術プロセッサを提供するものである。ＡＬＵは、オペランドデータを受信するオペランド入力データパスと、算術演算の結果を戻す結果データ出力パスとを有する。レジスタファイルはオペランドデータパスと結果データパスに結合されている。レジスタファイルは複数の算術回路によって共用されている。さらに、コントローラがＡＬＵおよびレジスタファイルに結合されていて、このコントローラは、算術演算を要求するモード制御信号に応答して、複数の算術回路の１つを選択し、レジスタファイルとＡＬＵとの間でデータアクセスを制御し、それによりレジスタファイルが算術回路によって共用されるようにする。

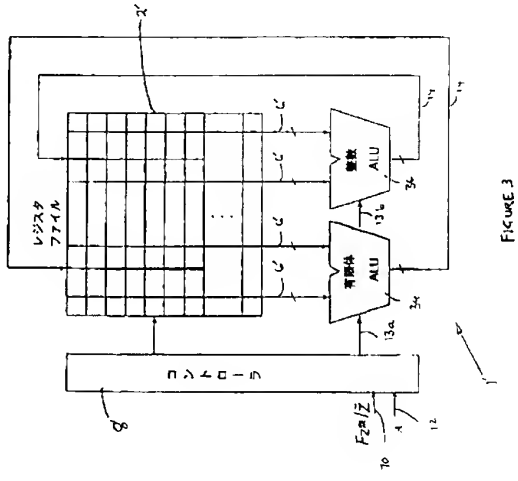


FIGURE 3

【特許請求の範囲】

１．（ａ）有限体算術演算をパフォームする有限体算術回路とモジュラ整数算術演算をパフォームするモジュラ整数算術回路を有する論理演算装置であって、オペランドデータを受信するオペランド入力データバスと前記算術演算の結果を戻す結果データ出力バスとを有する論理演算装置と、

（ｂ）前記オペランドデータバスおよび前記結果データバスに結合したレジスタファイルと、

（ｃ）前記ＡＬＵおよび前記レジスタファイルに結合したコントローラであって、モード制御信号に応答して前記有限体演算または前記整数算術演算のいずれかを選択し、前記レジスタファイルと前記ＡＬＵの間でのデータアクセスを制御して、前記レジスタファイルが前記有限体算術回路および整数算術回路の両方によって共用されるようにしたコントローラと

を備えたことを特徴とする算術プロセッサ。

２．請求項１において、

前記レジスタファイルは汎用レジスタを含み、

前記ＡＬＵは前記オペランドバスのデータビット幅より広い処理ビット幅を有すること

を特徴とする算術プロセッサ。

３．請求項１において、前記コントローラは、前記論理演算装置により選択された算術演算を制御する命令をプログラムしたことを特徴とする算術プロセッサ。

４．請求項１において、前記オペランドバスは、前記ＡＬＵの処理ビット幅および前記結果データバスのビット幅と同じビット幅を有することを特徴とする算術プロセッサ。

５．請求項４において、前記オペランドデータバスは、第１および第２のオペランドをそれぞれ前記ＡＬＵと結合する第１および第２のオペランドバスを含むことを特徴とする算術プロセッサ。

６．請求項５において、前記汎用レジスタは、

前記コントローラによって個別にアドレスすることができ、

前記ＡＬＵの前記処理ビット幅より大きな体サイズについて前記ＡＬＵで計算するために、複数のレジスタ中のデータを組み合わせる
ことができることを特徴とする算術プロセッサ。
７．請求項１において、前記コントローラが体サイズの制御に応答して、前記ＡＬＵが種々の体サイズに作用することができることを特徴とする算術プロセッサ。
８．請求項１において、
前記ＡＬＵは、
前記算術演算で利用するオペランドを前記レジスタファイルから受信する複数の特殊レジスタと、
前記特殊レジスタの１つ以上のビットを結合する組合せおよびロジック回路要素を有する複数のサブＡＬＵと、
前記コントローラから受信した制御情報に応答する順序づけコントローラとを含み、
前記順序づけコントローラ、ならびにその中のカウンタおよび検出回路は、前記特殊レジスタおよび前記複数のサブＡＬＵに結合され、算術演算中の一連のステップがパフォームされるようにその演算を制御する
ことを特徴とする算術プロセッサ。
９．請求項８において、前記ＡＬＵは、有限体の乗算と、二乗と、加算と、減算と、反転の前記算術演算をパフォームすることを特徴とする算術プロセッサ。
１０．請求項８において、前記サブＡＬＵは、ＸＯＲと、シフトと、シフトＸＯＲと、加算と、減算論理演算をパフォームすることを特徴とする算術プロセッサ。
１１．請求項１において、前記有限体算術回路は、
第１および第２のオペランドビットベクトルをそれぞれ受信するＡレジスタおよびＢレジスタと、モジュラスビットベクトルを受信するＭレジスタと、前記オペランドの有限体の積を含むアキュムレータとを含む複数の特殊レジスタを有する有限体乗算器回路と、

前記ＡおよびＢレジスタの各セルから前記アキュムレータのセルへの接続を確立するロジック回路と、

前記レジスタおよび前記ロジック回路に動作可能に接続され、前記有限体の積を得る一連のステップを実施する順序づけコントローラと

を含むことを特徴とする算術プロセッサ。

１２．請求項１１において、前記一連のステップは、

前記Ａレジスタの内容と前記Ｂレジスタの連続ビットの部分積を計算するステップと、

前記部分積を前記アキュムレータにストアするステップと、

前記部分積のビットを試験するステップと、

前記テストしたビットがセットされた場合に前記部分積を前記モジュラスで簡約するステップと、

前記Ｂレジスタの連続ビットについて前記ステップを繰り返すステップと

を備えたことを特徴とする算術プロセッサ。

１３．請求項１２において、

前記左そろえのオペランドベクトルを前記Ａレジスタおよび前記Ｂレジスタにそれぞれストアするステップを含み、

前記テストビットは前記レジスタの前記左端のビットから得られる

ことを特徴とする算術プロセッサ。

１４．請求項１２において、前記Ｂレジスタがシフトレジスタであることを特徴とする算術プロセッサ。

１５．請求項１４において、前記ロジック回路は、

レジスタセルA_iおよびアキュムレータC_iから得られる入力を有し、レジスタＢのセルB_{N-1}から得られた第１の加算制御信号に応答して第１の加算出力信号を生成する第１の制御可能加算器と、

モジュラスレジスタセルM_iおよび前記加算出力信号から得られる入力を有し、前記アキュムレータのセルC_{N-1}から得られた第２の加算制御信号に応答してアキュムレータセルC_iに結合される出力を生成する第２の制御可能加算器と

をそれぞれ含む、それぞれのレジスタセルに結合した複数の制御可能加算装置を有することを特徴とする算術プロセッサ。

１６．請求項１５において、有限体加算器回路を含むことを特徴とする算術プロセッサ。

１７．請求項１６において、前記有限体加算器は、レジスタＢの前記セルＢｉから得られた入力を前記第１の加算器それぞれに結合する手段と、前記第２の加算器の前記出力を前記セルＣｉに結合する手段とを含み、

前記順序づけコントローラが有限体加算制御信号に応答し、それにより前記有限体加算演算が１クロックサイクルでパフォームされる
ことを特徴とする算術プロセッサ。

１８．請求項１において、前記有限体算術回路は有限体反転回路を含むことを特徴とする算術プロセッサ。

１９．請求項１８において、前記有限体反転回路は、

第１および第２のオペランドビットベクトルをそれぞれ受信するＡレジスタおよびＢレジスタと、モジュラスビットベクトルを受信するＭレジスタと、前記オペランドの有限体の積を含むアキュムレータとを含む複数の特殊レジスタを備えたことを特徴とする算術プロセッサ。

２０．請求項１において、前記ＡＬＵは、

有限体乗算器回路と、

有限体反転回路と、

複数の特殊レジスタと、

前記特殊レジスタの各セルの間で接続を確立するロジック回路と、

前記レジスタおよび前記ロジック回路にアクション可能に接続され、有限体の積または有限体の反転を計算するための一連のステップを実施し、それにより前記特殊レジスタが前記有限体乗算器および前記有限体反転回路によって共用されるようにする、順序づけコントローラと
を備えたことを特徴とする算術プロセッサ。

２１．請求項２０において、前記有限体反転回路は、拡張したユークリッドの互

除法を実施することを特徴とする算術プロセッサ。

２２．請求項１１において、整数算術乗算回路を含むことを特徴とする算術プロセッサ。

２３．請求項１２において、前記整数算術乗算は、前記モード選択信号に応答して前記mレジスタに桁上げをロードすることによって実装されることを特徴とする算術プロセッサ。

２４．請求項１において、暗号化システムで使用されることを特徴とする算術プロセッサ。

２５．（ａ）一群の関連する算術演算をそれぞれパフォームする複数の算術回路を有するＡＬＵであって、オペランドデータを受信するオペランド入力データバスと、前記算術演算の結果を戻す結果データ出力バスとを有するＡＬＵと、

（ｂ）前記オペランドデータバスおよび前記結果データバスに結合したレジスタファイルと、

（ｃ）前記ＡＬＵおよび前記レジスタファイルに結合したコントローラであって、算術演算を要求するモード制御信号に応答して前記複数の算術回路の１つを選択し、かつ前記レジスタファイルと前記ＡＬＵの間でデータアクセスを制御し、それにより前記レジスタファイルが前記算術回路によって共用されるようにするコントローラと

を備えたことを特徴とする算術プロセッサ。

２６．請求項２５において、前記算術回路は、有限体算術回路およびモジュラ整数算術回路であることを特徴とする算術プロセッサ。

【発明の詳細な説明】

算術プロセッサ

本発明は、有限体および整数の算術をパフォームする方法および装置に関する。

発明の背景

有限体（finite field）に対するＥＣ（Elliptic Curve）暗号法では、加算と、乗算と、二乗と、反転（inversion）の算術演算が必要となる。さらに、体（field）の標数が２でない場合には、減算も必要になる。例えば符号定数の計算では、モジュラ算術演算も必要になるが、このような演算は有限体の演算ほど必要にならない。例えばＥＣ暗号法では、モジュラおよび有限体演算、加算、減算、乗算、反転の完全な補集合（full complement）が必要になる。

暗号法のための体のサイズは比較的大きくなる傾向があり、算術演算を許容時間内で実行するために高速の専用プロセッサが必要になる。したがって、高速モジュラ算術プロセッサか、Ｆ２ｎの算術演算をパフォームする専用プロセッサのいずれかが、多数インプリメントされている。特殊目的または専用プロセッサを使用することは、当技術分野では、周知のことである。こうしたプロセッサは一般にコプロセッサと呼ばれ、通常は、ホスト計算システムで利用されており、従って、命令および制御はメインプロセッサからコプロセッサに提供されている。

なかでもＲＳＡが暗号化システムとして慣用されていたが、優秀かつよりセキュアなＥＣ暗号法が登場したため、モジュラ冪法（modular exponentiation）専用のプロセッサの必要性は、薄らいで来ている。ユーザはＲＳＡ暗号法からＥＣ暗号法に移行しているものの、性能およびコストをほとんどあるいは全く犠牲にすることなくこれらの両方の演算をサポートする算術プロセッサに対するニーズがある。

発明の概要

本発明の第１の目的は、有限体算術と整数算術を組み合わせ、ＥＣ暗号法に必要な演算と、例えばＲＳＡ暗号法で必要なモジュラ冪法とを提供するプロセッサを提供することにある。

本発明の第２の目的は、異なる体またはレジスタサイズにスケーリングすることができる算術プロセッサ設計を提供することにある。

本発明の第３の目的は、異なる体サイズで使用することができる算術プロセッサを提供することにある。

本発明の第４の目的は、マルチシーケンス中の複数のステップを同時にパフォームすることによってマルチシーケンス演算実行を高速化するためにスケーリングすることができる算術プロセッサを提供することにある。

本発明によれば、

（ａ）一群の関連する算術演算をそれぞれ実行する複数の算術回路を有する論理演算装置であって、オペランドデータを受信するオペランド入力データバスと、前記算術演算の結果を戻す結果データ出力バスとを有する論理演算装置と、

（ｂ）前記オペランドデータバスおよび前記結果データバスに結合されたレジスタファイルと、

（ｃ）前記ＡＬＵおよび前記レジスタファイルに結合された制御装置であって、算術演算を要求するモード制御信号に応答して前記複数の算術回路の１つを選択し、かつ前記レジスタファイルと前記ＡＬＵの間でデータアクセスを制御することにより、前記レジスタファイルが前記算術回路によって共用されるようにする制御装置と

を含む算術プロセッサが提供される。

本発明の別の実施形態によれば、有限体回路および整数算術回路を含み、かつ汎用レジスタおよび専用レジスタを備えたプロセッサが提供される。

本発明の別の実施形態によれば、有限体算術および整数算術を両方とも実行し、専用レジスタおよび汎用レジスタの両方ならびに算術回路を共用する算術プロセッサが提供される。この目的のために、多項式基底が整数の標準的な基数累乗基底（standard radix-power basis）と同様であるので、有限体ハードウェアについて多項式基底を想定する。

図面の簡単な説明

以下、本発明の実施形態を、添付図面を参照し例を挙げて説明する。

図１は有限体算術および整数算術をパフォームする算術プロセッサアーキテクチャのブロック図である。

図２は図１に示すＡＬＵ（arithmetic logicunit）の概略ブロック図である。

図３は有限体算術および整数算術をパフォームする算術プロセッサアーキテクチャの代替実施形態のブロック図である。

図４は図３に示すＡＬＵの概略ブロッタ図である。

図５（ａ）、（ｂ）、および（ｃ）は図２に示すＡＬＵのビットスライスの実施形態のブロック図である。

図６は図５に示すビットスライスの有限体乗算器の回路図である。

図７は算術インバータのブロック図である。

図８は組み合わせた有限体／整数乗算器の回路図である。

図９は図１のマルチビットＡＬＵの実施形態を示す概略ブロック図である。

図１０は図９のマルチビット有限体乗算器の回路図である。

好ましい実施形態の詳細な説明

図１を説明する。算術プロセッサの一実施形態は一般的に参照番号１で示してある。当然のことであるが、この算術プロセッサは総合計算システム中の汎用プロセッサとともに使用することができ、データはこの計算システムと算術プロセッサの間で交換される。算術プロセッサには、レジスタファイルと呼ばれる一群の汎用レジスタ（ＧＰ）２が含まれている。レジスタファイルはＥＣの点加算（point addition）、点倍加（point doubling）などのための中間記憶域として使用することができるものである。一群の汎用レジスタ２はデータ入力またはオペランドバス６を介してＡＬＵ（arithmetic logicunit）４と通信を行なっている。ＡＬＵ４にはシェアード（shared）有限体および整数算術回路が含まれている。ＡＬＵ４による計算の結果をレジスタファイル２に書き込むため、データ出力または結果バス１４がＡＬＵ４とレジスタファイル２の間に設けてある。

ＡＬＵ４による計算オペレーションは、算術プロセッサ１のコントローラ８に

駐在するマイクロプログラム化命令により制御されている。モード選択コントロール１０は有限体計算またはモジュラ整数計算を選択するために用意してある。

体サイズ制御１２も、ＡＬＵ４を初期設定して、種々のオペランドベクトルサイズに適応させるために用意してある。そこで、コントローラ８はなかんずく次のタスク、すなわち、適正な算術モードおよび演算をＡＬＵ４に提供するタスクと、レジスタファイル２とＡＬＵ４の間のデータアクセスをコーディネートするタスクと、使用される適正な体のサイズをＡＬＵ４に提供するタスクとをパフォームする。

汎用レジスタは、少なくとも予想可能な最大のF_{2m}ＥＣ暗号システムをハンドルするだけのビット幅を有するように選択される。これら汎用レジスタは整数モジュラ算術で必要なビット長をサポートするために、組み合わせることができる。例えば、レジスタファイル２の単一レジスタのビット幅が５１２ビット幅である場合に、単一の２０４８ビットＲＳＡ量の記憶域を提供するため、４つのレジスタを使用することができる。これら汎用レジスタには、データのブロックがロードされ、例えば、２０４８ビットの計算をブロック単位で行い、ついで、再組み立てして、全幅結果（full width result）を得ることができる。典型的には、算術プロセッサ１は既存のホストコンピュータシステムで利用され、コントローラ８はこのホストコンピュータシステムから制御信号を受信し、適正なホストバスインタフェースを介して、ホストデータバスにデータを通信する。このようなインタフェースの詳細は当業者とって周知のことであり、説明は省略する。

図２を説明する。ＡＬＵ４には、幾つかの特殊レジスタ１６と、複数のサブＡＬＵ１８と、出力データバス３０と、コントローラ２０とが含まれている。複数のサブＡＬＵ１８には組み合わせロジックおよび算術回路が含まれていて、組み合わせロジックおよび算術回路は、特殊レジスタからデータバス２８を介して各サブＡＬＵに入力された１つ以上のビットをオペレートする。出力データバス３０はサブＡＬＵ１８と特殊レジスタとの間に設けてある。コントローラ２０は、なかんずく、次のタスク、すなわち、計算オペレーション中の各ステップを通してＡＬＵ４を順序づけるタスクと、特殊レジスタ１６からの制御ビットを監視するタスクと、使用してある体のサイズを決定するためにカウンタを制御レジスタ

２２に実装するとともに、プロセッサハードウェアを設計し直さずに、プロセッ

サ１が異なる体サイズに対して使用することができる機構を実装するタスクとをパフォームする。これらの機能を提供するため、特殊レジスタ１６の制御ビット２６は制御ビット入力２４としてコントローラ２０に供給される。特殊レジスタ１６は、全て、個別にアドレス可能になっている。コントローラ２０はレジスタファイルから入力バス６を介してサブＡＬＵ１８または特殊レジスタ１６に入力されたデータも制御する。これらサブＡＬＵは、単一のビットにオペレートすることができ、複数のビットに一度にオペレートすることができる。これらのコンポーネントは後程より詳細に記述する。

図３を説明する。算術プロセッサの代替例は参照番号１′で示してある。本実施形態では、別個の有限体装置３４および整数モジュラ算術装置３６を提供する。このプロセッサは、レジスタファイル２′と、データ入力バス６′と、データ出力バス１４′と、コントローラ８′も含むが、制御１３ａおよび１３ｂがそれぞれコントローラ８′から各ＡＬＵ３４および３６に提供される。

図４を説明する。図４は図３のＡＬＵ３４および３６をより詳細に示す。ＡＬＵ３４および３６には、それぞれ、特殊レジスタ１６′ａおよび16′ｂと、コントローラ２０′ａおよび２０′ｂとが含まれている。ＡＬＵ３４および３６には、それぞれ、サブＡＬＵ１８′ａおよび18′ｂが含まれている。したがって、この実施形態では、特殊レジスタ１６′ａおよび16′ｂと、算術および制御回路は、当然、共有されない。サブＡＬＵ１８′ａのうちの１つ以上のサブＡＬＵ１８′ａは、協働して、シフト左／右とＸＯＲシフトの機能を実行し、サブＡＬＵ１８′ｂのうちの１つ以上のサブＡＬＵ１８′ｂは、協働し、任意選択で、桁上げ保存技術または桁上げ伝搬（carry propagation）を使用して、整数加算および整数減算の機能を実行する。

図２を説明する。サブＡＬＵ１８は、特殊レジスタ１６から供給されたオペランドに対して、次の論理機能、すなわち、ＸＯＲと、シフト左／右と、ＸＯＲシフトと、整数加算と、整数減算を実行する。これらの機能は、１つのサブＡＬＵ１８か、マルチプル・サブＡＬＵに含めることができる。マルチプル・サブＡＬＵ１８を設けることにより、当該プロセッサは複数の演算（例えば、有限体反転）

を同時にパフォームすることができる。

図５を説明する。図５は図２のＡＬＵ４のビットスライス４１を詳細に示す。次の考察では、ビットスライス４１と関係付けをしたロジッタ回路と関連して、各特殊レジスタのセルを相互接続する、と言う。ビットスライスに含まれたロジック回路は、一般的に、図２に示すようなサブＡＬＵ１８のうちの１つで表される。ビットスライスの構成は、Ｎビットレジスタに対しては、Ｎ回繰り返えすことができる。さらに、明確にするため、Ｎをレジスタ内のセル数と定義し、レジスタ内の個別のセルを例えばA_iという。ここで、$0 \leqq i \leqq N-1$であり、A_{N-1}は特殊レジスタの最も右にあるセルである。レジスタの内容は小文字で参照され、例えば、長さｎのビットベクトルＡは、a_0をＬＳＢとして、ビットにa_0, …a_{n-1}と番号が付けられることになる。ここで、特殊レジスタには特定の名前が付けられているが、これらのレジスタは、後程説明するが、実行されている算術演算に依存して異なる機能をとることができる、ことに留意されたい。

図５の特殊レジスタ１６に含まれるレジスタとしては、乗算演算中に、例えば、被乗数および乗数を個々に保持するための一対のオペランドレジスタＡ４２およびＢ４４と、累算器レジスタＣ４６と、モジュラスレジスタＭ４８と、桁上げ拡張（carry extension）レジスタC^{ext}５０（整数算術で使用される）とがある。

これらのレジスタは、その中にロードされたビットベクトルの個々の２進数を保持するため、Ｎ個のセルを有する。これらのレジスタはシフトレジスタであるのが好ましい。図２に示すサブＡＬＵ１８は、後程説明するが、図５のブロック５２の回路により実装することができる。

乗算

ＡＬＵ４のオペレーションは、有限体乗算のような具体的な算術演算を参照することにより最も良く理解することができる。ここで、２つの元ａおよびｂの積Ｃを考察することにする。ここで、ａおよびｂはビットベクトルであり、ｂは多項式表現でｂ＝（b_0, …b_{n-1}）の形態となり、ａは多項式表現でａ＝（a_0, …a_{n-1}）の形態となる。モジュラスビットベクトルｍは、ｍ＝（m_0, …m_n）の形態を有する。モジュラスレジスタは、モジュラスを表すのに必要なビット数

より

１ビット多い、ことに留意されたい。あるいはまた、最上位ビットm_nが１であるので、この最上位ビットを暗黙に定義することができ、mを（m_0，…m_{n-1}）で表すこともできる。$F2^n$において、乗算は、次のような疑似コードにより明確に記述される一連のステップとして実装することができる。

C＝０ {C_{-1}＝０}

For i from n-1 to 0 do

For j from n-1 to 0 do {$C_j=C_{j-1}+b_j a_j+c_{n-1}m_j$}

この乗算を実行する際には、ＭＳＢ（most significant bit）からＬＳＢ（least significant bit）の順に、被乗数と乗数のb_iの各ビットとの部分積を形成する。その前の部分積のＭＳＢがセットされた場合には、部分積はモジュラスによって簡約（reduce）される。

乗算の実装は、１×Ｎ乗算器を逐次使用することによって行なうことができ、この場合、上記疑似コードの内側の「ｆｏｒ」ループはパラレルに実行される。各セルがそれぞれ２進数m_iの１つを含むように、モジュラスレジスタＭには、ＭＳＢm_nを剥ぎ取ったモジュラスビットベクトルmがロードされる。図示の実装では、ビットm_iは、ベクトルのＭＳＢを最も左側のビットとして、左から右に配列されている。すなわち、セルM_{n-1}はビットm_{n-1}を含む。Ｎ≠ｎである場合、スティルビット（still bit）M_{n-1}はM_{N-1}にストアされる、すなわち、データは左寄せされる。各セルが個々に２進数a_iまたはb_iの１つを含むように、シフトレジスタＡおよびＢには、有限体元（finite field element）ビットベクトルａおよびｂがそれぞれロードされる。有限体元ａおよびｂは、左寄せされ、各レジスタにストアされ、乗数レジスタｂのＭＳＢが常に左境界セルのビット、すなわち（a_{n-1}，a_{n-2}，…a_0）および（b_{n-1}，b_{n-2}，…b_0）で利用可能になっている。ベクトルａおよびｂの長さがレジスタの長さより短い場合には、残りのセルには０がパディングされる。以上、図２に示すコントローラ２０によって一般的に実行される。逐次乗算（被乗数を逐次小さくするなど）の他の構成も可能であるが、そのような構成では、体のサイズに柔軟性を持たせることができ

ないし、同様に、制御ビット位置を固定することができない。この乗算アルゴリズムを対応して変化させれば、ＬＳＢからＭＳＢへのビット順序づけも可能である。

ここでは、ＡＬＵ４のビットスライス４１は、有限体において乗算を実装するために、記載されている。ビットスライス４１は第１および第２のコントローラブル加算器５４および５６を含み、第１および第２のコントローラブル加算器５４および５６は、それぞれ、ＸＯＲ機能を有する。レジスタＢの最上位のセルB_{N-1}は、加算制御信号b_{n-1}５７を第１の加算器５４に供給する。第１の加算器５４への入力５８および６０は、レジスタセルA_iおよびアキュムレータセルC_iから得られる。第１の加算器５４からの出力６２は、モジュラスレジスタセルM_iからの入力６４とともに、第２の加算器５６の入力に接続されている。加算器５４は出力６２＝入力６０＋（入力５８および制御５７）という演算をパフォームする。この演算を図５（ｂ）に詳細に示す。

ついで、第２の加算器５６からの出力はアキュムレータセルC_iに接続されている。第２の加算制御信号６６はアキュムレータＣ４６の最上位のセルC_{N-1}から得られる。アキュムレータＣの最上位のビットC_{N-1}がセットされたとき、当然に、モジュラスベクトルｍによるアキュムレータＣでの部分積のモジュラ簡約が、第２の加算制御信号６６により実装される。図５（ｃ）に詳細に示すように、加算器５６は、出力＝入力６２＋（入力６４および制御６６）という演算を行う。Ｂレジスタはクロックシフトレジスタである。コントローラ２０から供給することができるクロック信号ＣＬＫ１　６８は、部分積が計算される度に、このレジスタの内容を左にシフトさせる。

図６を説明する。図６は図５のビットスライス４１の詳細な回路実装を示す。この回路実装は有限体乗算を行なうためのものであって、参照番号７０で示す。図６のビットスライスｉ、７０を説明する。図６では、説明のために、ビットスライスは３つしか示していない。セルa_iは、ＡＮＤゲート７２により、加算制御信号b_{n-1}とＡＮＤ演算される。ＡＮＤゲート７２の出力７４は、アキュムレータＣの隣接するセルＣｉ－１からの入力７８とともに、ＸＯＲゲート７６の入

力に接続される。よって、項「$c_{j-1}+b_i a_i$」の計算が実装される。項「$c_{n-1} m_j$」は、ＡＮＤゲート８４を利用して、信号c_n８０とm_i８２をＡＮＤ演算することにより、実装される。ＡＮＤゲート８４の出力８６は、ＸＯＲゲート７６の出力８８とともに、ＸＯＲゲート８４の入力に接続される。ＸＯＲゲート８４

の出力９０は、セルC_i９２に接続される。よって、式「$c_j = c_{j-1}+b_i a_i + c_{n-1} m_j$」が実装される。この汎用の逐次乗算器により、２つのｎビット有限体元の積がｎクロックサイクルで生成されることになる。同期カウンタは、コントローラ２０に含めることができるものであって、繰返し回数の制御を行うものが好ましい。以上の記述は、加算器５４が整数加算器のビットスライスであって、加算器５６が整数減算器のビットスライスであるときに、整数モジュラ乗算に適用される。このことは後程説明する。

<u>加算</u>

有限体$F 2^n$中の乗算に関連して、回路を説明したが、その他の計算オペレーションも容易にパフォームすることができる。有限体加算は桁上げが生じないので、この点で、整数算術より有利である。有限体サム（sum）の計算では、有限体中の２つの元ａおよびｂの加算が、単に、ａとｂのＸＯＲであるので、ＸＯＲゲートを注目レジスタの各セルに導入するだけでよい。したがって、図５に戻ると、入力１００はセルＢｉから第１の加算器５４に供給され、第２の加算器５６は簡約に使用される。ついで、加算器５４からの出力はセルC_iに直接書き込まれる。オペランドがレジスタａおよびｂに移動された後で、単一のクロックサイクルで、加算をパフォームすることができる。その加算をＡＬＵでパフォームするのは可能であり、その結果をレジスタファイルの汎用レジスタにライトバックするのも可能である。整数加算では、加算器５４は整数加算器のビットスライスであり、整数加算結果に基づきモジュラオーバフローか否かを検査しなければならない。この状態が生じた場合には、整数減算器のビットスライスである加算器５６は、その結果を簡約するのに用いられる。

<u>二乗</u>

ある数を二乗するには、異なる２つの数の乗算と同じ時間でパフォームするこ

とができる。多項式基底における二乗は、特定の既約（irreducible）が二乗展開と明示的に結線された（hardwired）場合は、単一のクロックサイクルでパフォームすることができる。あるいはまた、同じ入力を乗算して二乗をパフォームする

ことができる。

反転

Ｆ２^{n}の有限体元の反転は、ユークリッドの互除法を使用してパフォームすることができ、また、追加のコントロールロジックを有する４つの特殊レジスタを利用してパフォームすることができる。この反転は、シフトが加算と同時に行われる場合（これは加算の出力を次のレジスタセルに結線することによって容易に実装される）には、２ｎサイクルで完了する。

この反転で使用されるレジスタは、Ａ、Ｂ、Ｍ、およびＣである。便宜上、これらのレジスタを概略的に図７に示す。ＭにはＵＬ、ＣにはＬＬ、ＡにはＵＲ、ＢにはＬＲとラベル付けがしてある。再度、この反転を、ビットスライス１１０に関連して記述することができる。

反転のオペランドは、一般に、反転する元ｇと、既約多項式ｆまたはモジュラスm（後述）と、ビットベクトル「０」と、ビットベクトル「１」である。ＵＬレジスタ１１６にはｆまたはmがロードされる。ＬＬレジスタ１１８にはｇがロードされ、ＵＲレジスタ１１２には「０」が、ＬＲレジスタ１１４には「１」がロードされる。ＵＲレジスタ１１２およびＬＲレジスタ１１４では、セルＵＲ$_{i}$およびＬＲ$_{i}$はＸＯＲゲート１２０でＸＯＲ演算されて、出力１２２が生じる。制御信号１２４は、可能な３つの入力のうち１つがセルＵＲ$_{i}$およびＵＬ$_{i}$に書き込まれるかどうかを決定する。入力は隣接するセルまたは出力１２２からの左または右シフトである。制御信号Ｂは後程記載する状態表によって決定される。ＵＬレジスタ１１６またはＬＬレジスタ１１８では、セルＵＬ$_{i}$およびＬＬ$_{i}$はＸＯＲゲート１２６でＸＯＲ演算されて、出力１２８が生じる。制御信号１３０は、可能な２つの入力のうち１つがセルＵＬ$_{i}$およびＬＬ$_{i}$に書き込まれるかどうかを決定する。入力は隣接するセル（ｉ－１）または出力１２８からの左シフトであ

る。この場合も、制御信号１３０は後程記載する状態表によって決定される。

制御変数をＵＬレジスタの長さk_uと、ＬＬレジスタの長さk_lと仮定したとすると、$\Delta = k_u - k_l$となる。値k_lおよびk_uは、好ましくは、同期ダウンカウンタで実装され、Δは好ましくは同期アップ／ダウンカウンタで実装される。カウンタレジスタk_u、k_l、およびΔも用意されている。ＵＬおよびＬＬレジスタは左シフトレジスタであり、ＵＲおよびＬＲレジスタは、ともに、左および右シフトレジスタである。

さらに、カウンタレジスタでは、Δには０がロードされ、k_uはｎに初期化される。制御ビットラッチは、「１」がアップカウントを示し、「０」がダウンカウントを示すトグル機能を有する。Ｕ／Ｄ制御は、最初、「１」にセットされる。この場合、ＡＬＵで反転を実行する制御装置に含まれるシーケンサは、次のような出力を有する。

deckl	デクリメントk_l　ｋｌ
decku	デクリメントk_u　ｋｕ
decDelta	デクリメントΔ
incDelta	インクリメントΔ
toggle	トグルアップ／ダウン
lsUL	左シフト左上レジスタ
lsLL	左シフト左下レジスタ
lsUR	左シフト右上レジスタ
lsLR	左シフト右下レジスタ
rsUR	右シフト右上レジスタ
rsLR	右シフト左下レジスタ
outLR	出力右下レジスタ
outUR	出力右上レジスタ
dadd-lsLL	ダウンＸＯＲおよび左シフト左下レジスタ
uadd-lsUL	アップＸＯＲおよび左シフト左上レジスタ

インバータのオペレーションの概要を表す状態表は次のようになっており、Ｍ

$_u$およびＣ$_l$はそれぞれレジスタＵＬおよびＬＬの上位ビットであり、Ｍ$_u$およびＣ$_l$は現在の状態を決定する。レジスタおよびカウンタ上でアクションがパフォームされると、これによりインバータは新しい状態となる。このプロセスは、ｋ

$_u$またはｋ$_l$が０になるまで繰り返され、右レジスタＲＬまたはＲＵの一方はg^{-1}を含み、もう一方はモジュラス自体を含むことになり、これは、後続の乗算または反転演算で使用するために、レジスタｍにリストア（restore）することができる。

U/D	k_u	k_l	Δ	M_u	C_l	アクション
X	0	X	X	X	X	OutLR
X	X	0	X	X	X	OutUR
1	$\bar{0}$	$\bar{0}$	0	0	1	$Deck_u$,dec Δ ,lsUL ,lsUR, toggle
1	$\bar{0}$	$\bar{0}$	$\bar{0}$	0	1	$Deck_u$,dec Δ ,lsUL, rsLR
0	$\bar{0}$	$\bar{0}$	X	0	1	$Deck_u$,dec Δ ,lsUL, lsUR
0	$\bar{0}$	$\bar{0}$	0	1	0	$Deck_l$,inc Δ ,lsLL,lsLR, toggle
0	$\bar{0}$	$\bar{0}$	$\bar{0}$	1	0	$Deck_l$,inc Δ ,lsLL,rsUR
1	$\bar{0}$	$\bar{0}$	X	1	0	$Deck_l$,inc Δ ,lsLL,lsLR
0	$\bar{0}$	$\bar{0}$	0	1	1	$Deck_l$,inc Δ ,Dadd-lsLL, lsLR, toggle
0	$\bar{0}$	$\bar{0}$	$\bar{0}$	1	1	$Deck_l$,inc Δ ,Dadd-lsLL, rsUR
1	$\bar{0}$	$\bar{0}$	0	1	1	$Deck_u$,dec Δ,Uadd-lsUL, lsUR, toggle
1	$\bar{0}$	$\bar{0}$	$\bar{0}$	1	1	$Deck_u$,dec Δ,Uadd-lsUL, rsLR

整数算術

多項式表現と整数表現は非常に良く似ていることから、ＡＬＵでハードウェアを共有することが可能でなる。加算では、整数算術は、桁上げが必要であることから、複雑になるだけである。ＡＬＵの整数算術演算は、例えば乗算演算を利用すれば、最もよく説明することができる。

疑似コードで表した次の一連のステップを参照して、Ｚにおける乗算を説明する。前述したのと同様に、ａおよびｂは乗算されるビットベクトルであり、ｃは

ａとｂの積であり、ｃ＝（c_0, c_1, …, c_{n-1}）である。

C＝0

M＝0

For i from 0 to n-1 do

$C^{ext} \leftarrow C$

For j from 0 to n-1 do

$C_j = (b_i (a_j) + m_j + c_j) \bmod 2$

$M^{j+1} = (b_j (a_j) + m_j + c_j) / 2$

ここで、

For i from 0 to n-1 do

$C^{cxt} \leftarrow C$

に対して、

$c_{j-1} = c_j$

$c_{j-1}{}^{ext} = c_j{}^{ext}$

となる。

同様に、このようにすれば、ＸＯＲを減算器で置換し、しかも、ｍレジスタに素数をロードした場合には、整数modulo ｐ（integcrs modulo p）を反転させることができる。改善策であるが、桁上げ保存方法を採用することにより、桁上げ伝搬を遅らせることができる。

図６の実施形態で説明した有限体乗算の場合のビットスライス７０を修正して、整数表現に対する乗算を含むようにすることができる、ことを観測することができる。注意すべきことであるが、整数乗算では、レジスタには、ビットベクトルがF_2mとは逆順でロードされる、すなわち、レジスタの最左端のセルがビットベクトルのＬＳＢを含む。整数乗算では、逐次（successive）部分積の間で、桁上げを実装する必要があり、さらに、部分積がモジュラスで簡約されていないので、逐次部分積の加算による桁上げを供給しなければならない。そこで、アキュムレータレジスタＣが拡張してあり、図５に示すように、新しいレジスタC^{ext}４９が設けてある。各部分積が形成される前に、アキュムレータＣの最下位ビッ

ト（セルC_M）を拡張レジスタC^{ext}の最上位ビット（セルC^{ext}_l）にシフトし、ついで、アキュムレータCおよびC^{ext}は両方ともＬＳＢに向けて１ビットだけシフトされる。最終結果はCおよびC^{ext}で獲得され、C^{ext}には、当該積の低位ビットが含まれる。このことは、上記オペレーション$C^{ext}\leftarrow C$で表される。

図８を説明する。図８はビットスライス１７０を示す。ビットスライス１７０は図６のビットスライス７０に類似している。したがって、同様のコンポーネントは、識別するために、図６の説明で使用した参照番号を１００番台にして使用することにする。つまり、参照番号７０は１７０となる。図８の編成が図６と異なる点は、モジュラスレジスタmが桁上げレジスタとして使用され、モード選択信号Ｚ／F_2m１７１が提供されるという、２つの重要な点である。

ここで、項$c_j = c_{j-1} + b_i a_i + c_{n-1} m_j$は、既に説明した有限体乗算でそうであったように、制御信号bmとレジスタセルA_iの内容との積で実装され、この積はＡＮＤゲート１７２で実装される。ＡＮＤゲート１７２の出力１７４はレジスタセルc_{j-1}の内容とＸＯＲゲート１７６によりＸＯＲ演算され、参照番号１５８で示す出力項$c_{j-1} + b_i (a_i)$が生成される。この出力信号は、ＡＮＤゲート１６０から得られた参照番号１８５で示す項$c_{n-1} (m_j)$と、ＸＯＲゲート１８４を使用してＸＯＲ演算され、項c_jが生成される。さらに、積$b_i a_i$, c_{j-1} １６２と、積$(c_{j-1} + b_i a_i, m_j)$ １６３とのサム（sum）から、桁上げ項m_iが生成され、セルm_i１８２に書き込まれる。積の項１６２および１６３はＡＮＤゲート１６４および１６６によってそれぞれ実装される。積の項１６２と１６３のサムはＯＲゲート１６７によって実装される。

モード選択信号Ｚ１７１は、桁上げ入力信号C_n１８０とＯＲ演算され、クロック信号１６９とＡＮＤ演算１６８される。したがって、Ｚ＝０をセットすることにより、有限体算術が実装され、Ｚ＝１をセットすることにより、整数算術が実装される。

図８は、図６で既に説明した有限体乗算を、組合せ有限体／整数乗算器に変換するのに必要な修正を示す。乗算の低位のビットを集めるため、出力レジスタCが拡張されることに留意されたい。Ｚにおける計算はモジュラスなしでパフォームされるので、モジュラスレジスタＭは、部分積を簡約するためではなく、桁上

げのホルダとして使用される。制御信号Ｚ／$Ｆ_{2}^{M}$１７１は、ＡＬＵのための整数乗算回路をイネーブルにする。

最終桁上げ伝搬（final carry propagation）は、マンチェスタリップルチェーン（Manchester ripple chain）によって提供することができ、レジスタ長が長いことから、１レイヤまたは２レイヤの桁上げスキップ機構によって拡張可能である。さらにｎサイクルだけクロックすることも可能であり、桁上げ保存加算器が桁上げを完全にマージすることが可能である。

１つの入力はその入力において条件付きで補数をとることができ、しかも、加算器のＬＳＢで「ホット」キャリインが行われる場合には、２の補数の減算は、桁上げ伝搬加算器で実装することができる。

乗算時のリップル桁上げは、桁上げスキップにより改良したとしても、許容できなくなるが、この桁上げ伝搬は、桁上げ保存加算器を使用すれば、ほぼ完全に除去することができる。このようにすると、部分積が冗長表現されるが、乗算が完了した後は解決される。

さらに別の実施形態では、ＡＬＵ４は、図９に示すように、計算速度が線形に増加するように修正することができる。これは、特殊レジスタ１６′からの連続ビットを一度に処理し、修正したサブＡＬＵ１９０で示す追加回路を実装し、図９に示すようにインクリメント加算を処理することによって達成される。複数のビットを処理すると、速度が線形増加することになる。例えば、計算が順次にパフォームされる場合は、その順序中の２つ以上のステップを同時に実行することができる。この場合、コントローラ２０′は特殊レジスタ１６′からの２ビット以上の制御ビット１９４を処理することになり、制御装置の入力１９２は図９にマルチビットラインとして示す。

有限体に対して一度に２ビット実行する乗算器(two-bit at a time multiplier)の回路図を図１０に示す。この実装では、ビットスライス２００はその数がＸＯＲゲート２１０の数の２倍であり、当該加算の２つの項を実装している。この乗算器は乗数から２ビットをとり、被乗数a_{i}およびa_{i-1}を２回だけ隣接してシフトすることにより加算し、モジュラスM_{i}およびM_{i-1}を２回だけ隣接してシフトすることにより簡約する。このようにすると、モジュラス簡約（modulus

reduction）で連続する２つの部分積が同時に生成され、したがって、全計算時間を半分にすることができるという効果がある。

特殊レジスタの上位（top）ビットがコントローラ２０または２０′用の制御ビットとして使用される、ことに留意されたい。このようにすると、オペランドがレジスタにロードされると、左揃えされ、したがって、制御が常に固定ビット位置から得られるという利点がある。しかし、その他のビット例えば下位（bottom）ビットを制御ビットとして使用することもできる。しかし、このようにすると、ハードウェアが複雑になることもある。

この場合も、Booth（または、修正Booth）記録などのオプションが可能となるので、マルチビット演算の計算速度がさらに線形的に増加する。

このようなＡＬＵは汎用レジスタに対して簡単な算術演算をパフォームする能力を有するものと仮定している。他の例のＡＬＵは全ての算術をＡＬＵ内部レジスタに対してパフォームするものであり、汎用レジスタはこれらのレジスタとの間でリード（read）およびライト（write）のみを行う能力を有する。

このようなＡＬＵの機能には、リップル桁上げや、桁上げスキップ加算と桁上げ完了の組合せなど、何らかの桁上げ伝搬方法を利用した、整数加算が含まれる。

このようなＡＬＵは、有限体加算で使用される単純なＸＯＲ機能も提供する。整数および有限体表現（ビット順序）が逆であるので、体から整数への変換と、整数から体への変換に使用されるビット逆転（bit reversal）機構を設けると有利である。２つのシフトレジスタの頂部どうしを接続することにより、ｎクロックサイクルでこの機能が提供される。ここで、ｎは算術オペランドの長さである。

本明細書で与えた一般的なアーキテクチャは、ＥＣとモジュラ指数算術との間でレジスタファイルを共用するだけでなく、共用制御レジスタに加えて、特殊レジスタおよび組み合わせロジックも共用する可能性がある。

以上、本発明の具体的な実施形態と具体的な用途について説明したが、種々の修正は、本発明の範囲を逸脱しない限り、当業者にとって可能である。例えば、

記載の実施形態では、特定のロジック回路について言及したが、例えば、ド・モルガンの法則を使用して等価な回路を使用することもでき、反転ロジック（inverted logic）が実装された場合には、相補形回路を使用することもできる、

ことに留意されたい。さらに、レジスタおよびビットベクトルのオリエンテーション、すなわち、左、右、上、下には、これらの方向の他の編成も含まれる。

本明細書で採用した項および式は、これらのものに限定されるものではなく、例として使用したものであり、これらの項および式を使用したことに、図示および記述した機構またはその一部分の均等物を排除する意図はなく、本発明の範囲内で種々の修正が可能であることを認識されたい。

【図１】

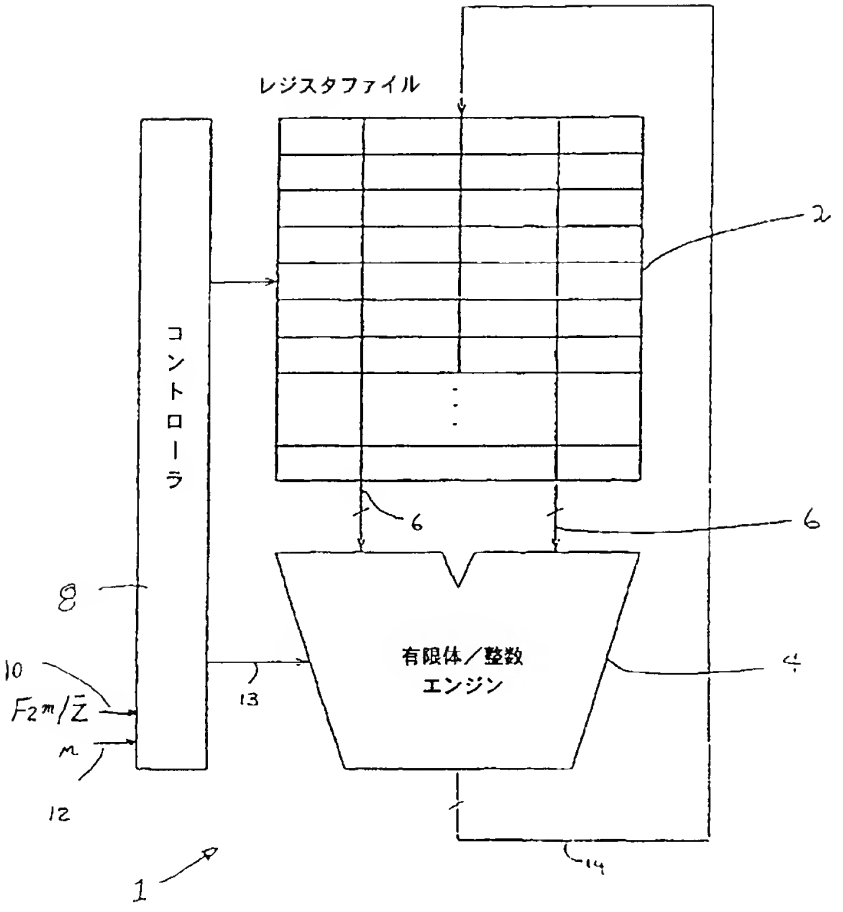


FIGURE 1

【図２】

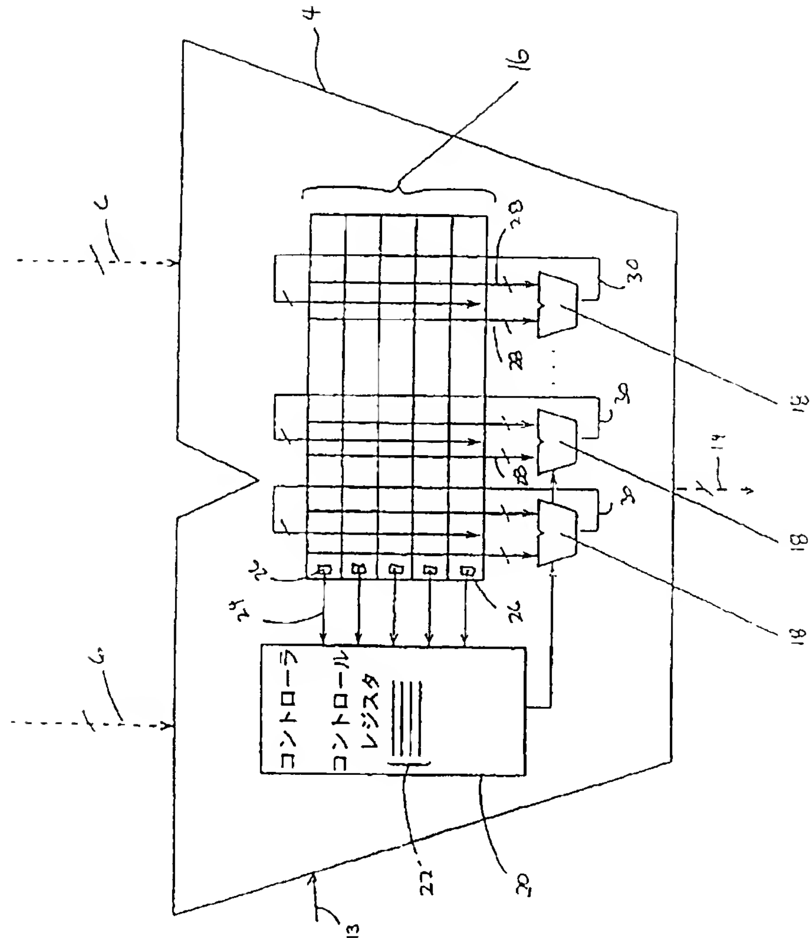


FIGURE 2

【図３】

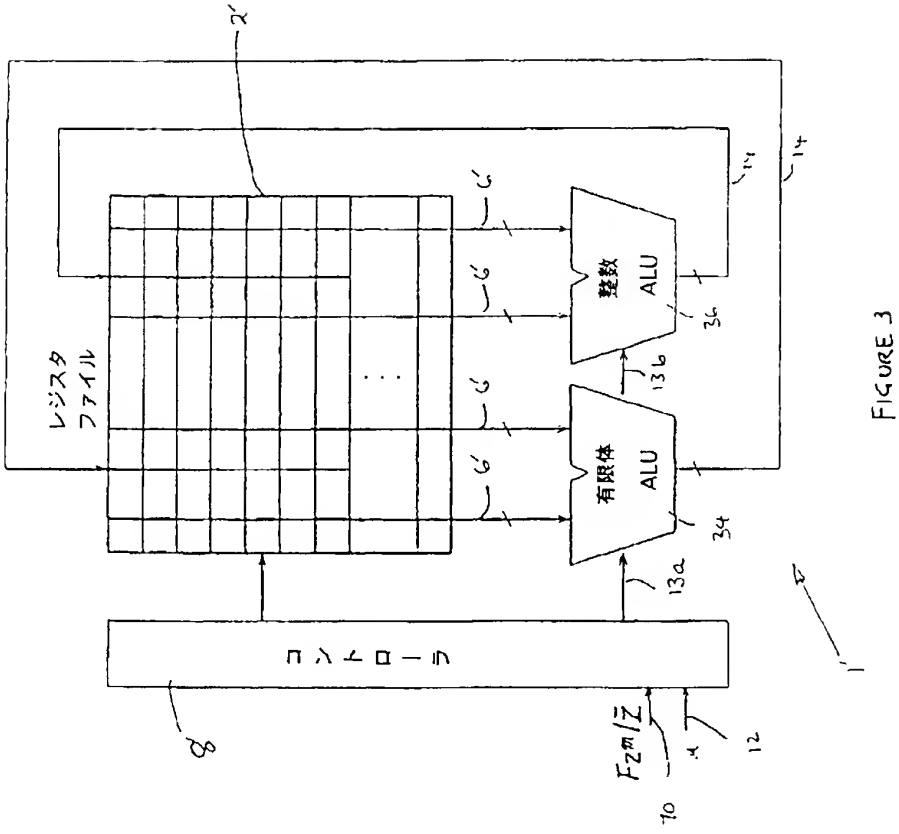


FIGURE 3

【図４】

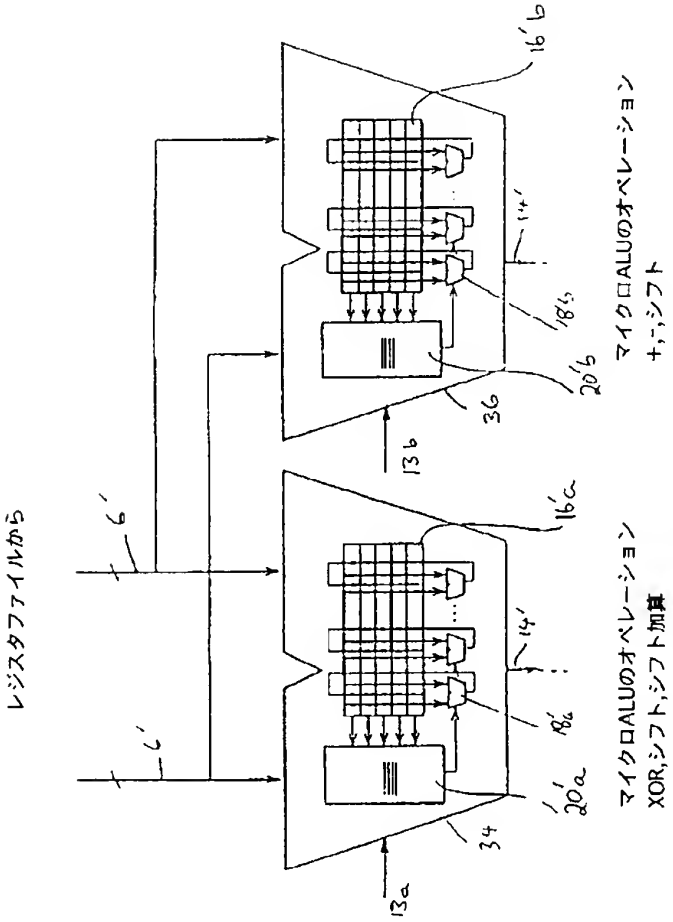

レジスタファイルから
6'
7'
16'b
16'a
14'
18'b
18'a
20'b
20'a
34
36
13a
13b
マイクロALUのオペレーション
XOR,シフト,シフト加算
マイクロALUのオペレーション
+,-,シフト

FIGURE 4

【図５】

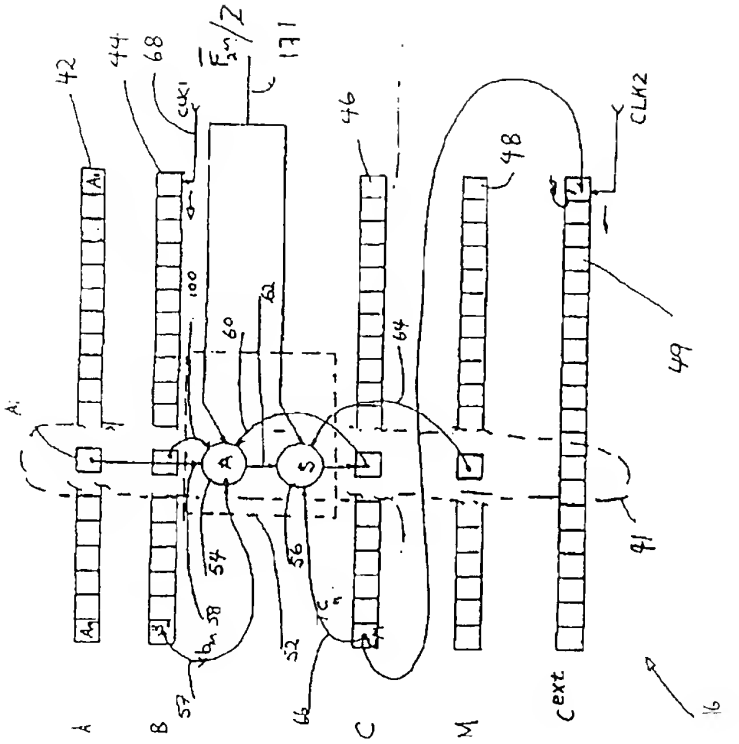
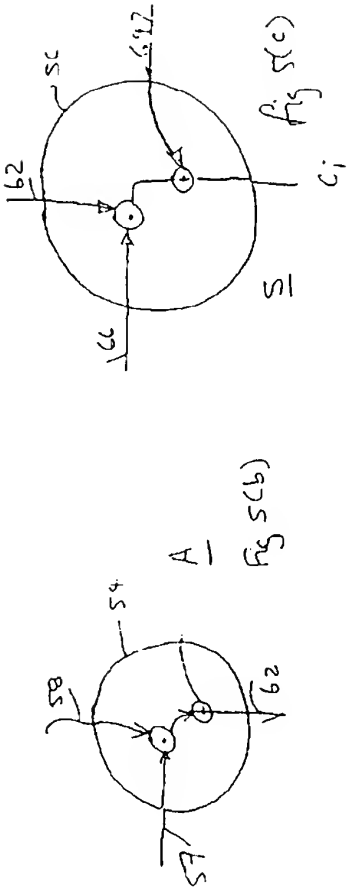

42
44
68
CLK1
171
46
48
CLK2
49
41
100
60
62
64
54
56
58
52
A
B
C
M
Cext
16

FIGURE 5(a)

【図５】



【図６】

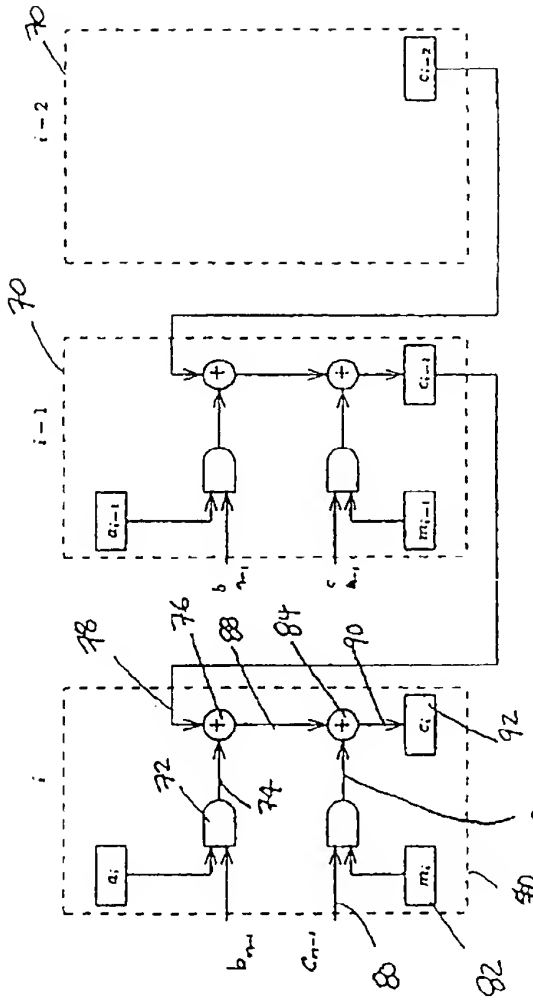

70
i-2
c_{i-2}
70
i-1
c_{i-1}
a_{i-1}
m_{i-1}
b_{n-1}
c_{n-1}
78
76
88
84
90
92
72
74
86
i
a_i
m_i
b_{n-1}
c_{n-1}
80
82
70

Figure 6

【図７】

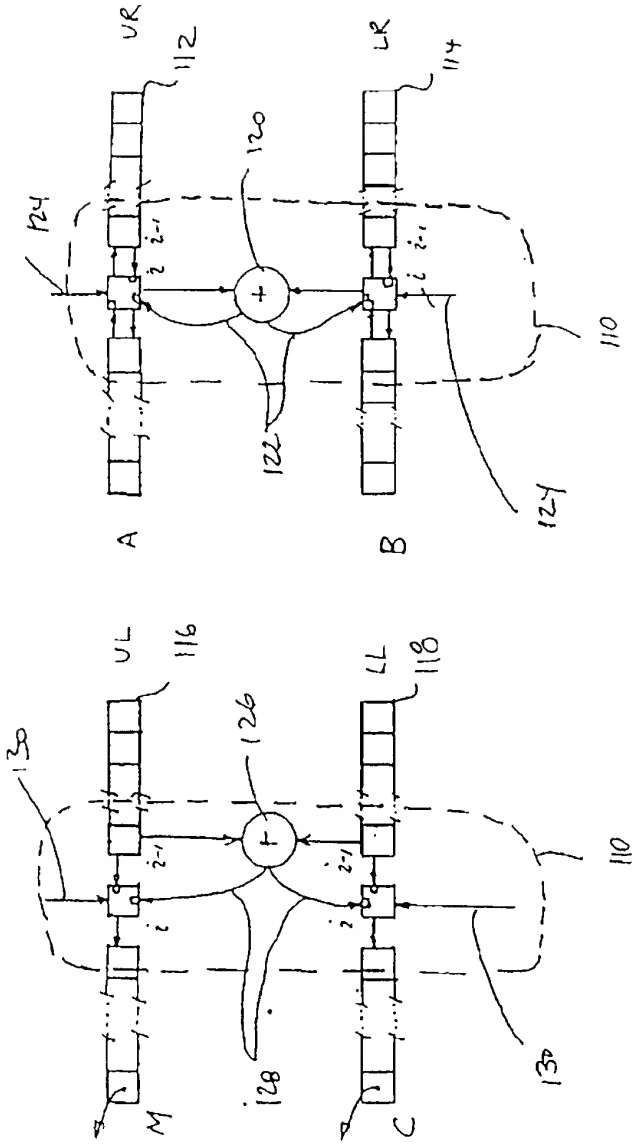
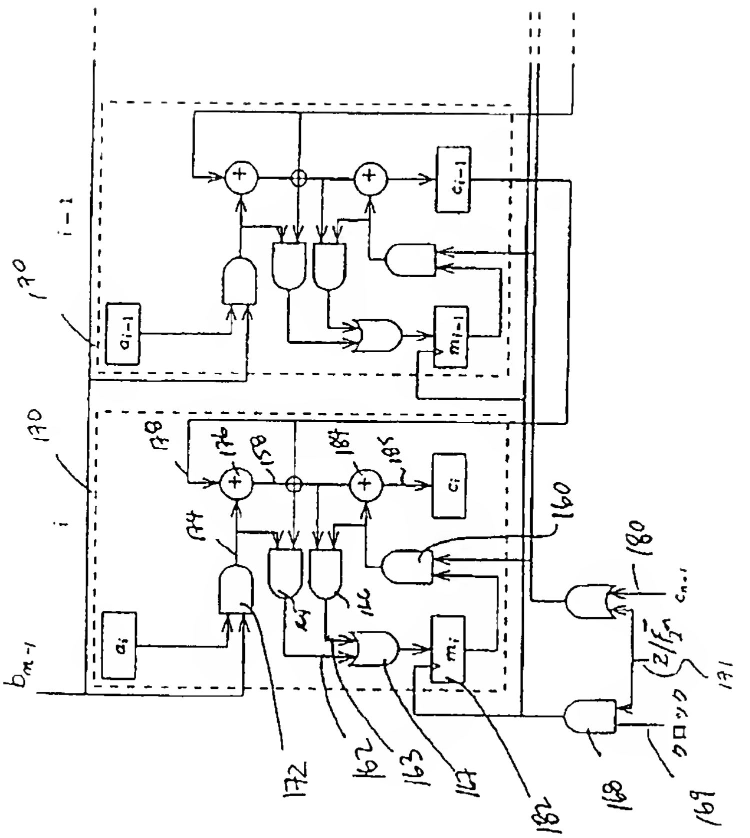


FIGURE 7

【図８】



170
170
i
i－1
a_i
a_{i-1}
c_i
c_{i-1}
m_i
m_{i-1}
b_{m-1}
クロック
160
180
171
172
162
163
167
182
168
169

Figure 8

【図９】

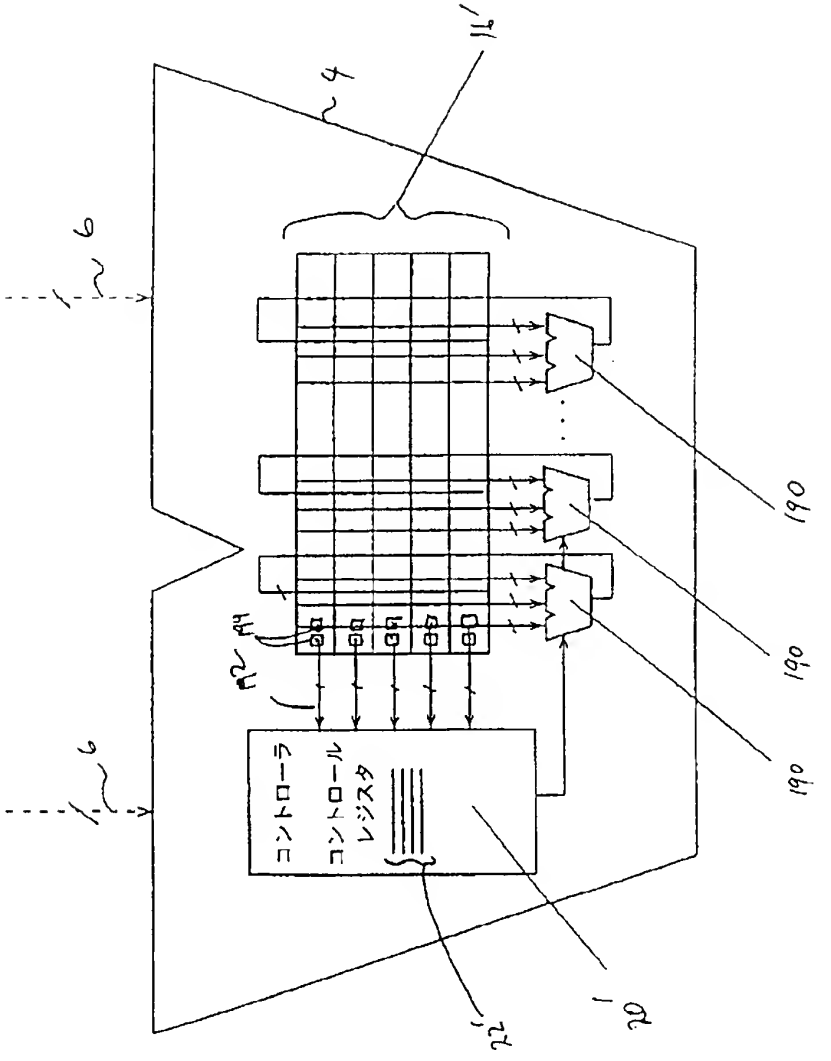


FIGURE 9

【図１０】

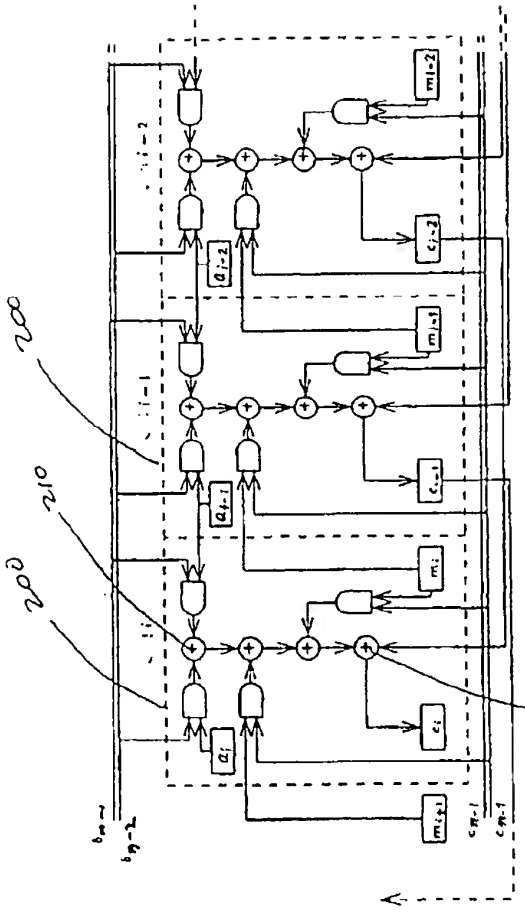


Figure 10

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/CA 98/00467

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F7/72

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 268 854 A (IKUMI NOBUYUKI) 7 December 1993 see column 1, line 45 - column 2, line 8; figure 9	25
A	US 5 459 681 A (HARRISON CALVIN W ET AL) 17 October 1995 see column 1, line 37 - line 46	1,26
A	EP 0 267 836 A (THOMSON CSF) 18 May 1988 see figure 1	1,26
A	FUCHS K C: "CRYPTOGRAPHIC SIGNAL PROCESSOR" MOTOROLA TECHNICAL DEVELOPMENTS, vol. 27, 1 May 1996, page 81/82 XP000594566 see the whole document	1,26

☐ Further documents are listed in the continuation of box C

☒ Patent family members are listed in annex

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 August 1998	13/08/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax. (+31-70) 340-3016	Verhoof, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

.nformation on patent family members

Int onal Application No
PCT/CA 98/00467

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5268854 A	07-12-1993	JP 2054544 C	23-05-1996
		JP 4178785 A	25-06-1992
		JP 7085267 B	13-09-1995
US 5459681 A	17-10-1995	NONE	
EP 0267836 A	18-05-1988	FR 2605818 A	29-04-1988
		DE 3778649 A	04-06-1992
		US 4888778 A	19-12-1989

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

(72)発明者 ガラント，ロバート．
カナダ エル７アール ２エヌ３ オンタリオ バーリントン パール ストリート 607―478

(72)発明者 ユリシク，アレクサンダー．
スロヴェニア共和国 1000 リュブリャーナ ビパブスカ 24エイ

(72)発明者 バデカール，アショク，ヴィ．
カナダ エル５アール ３ジー８ オンタリオ ミシソウガ カンスタレーション ドライブ 2006―700